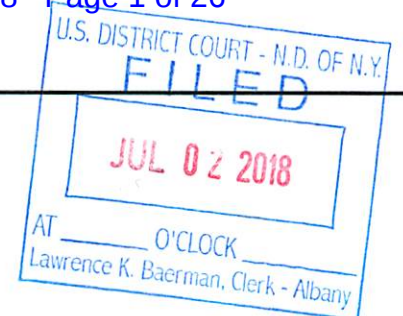


AO 106 (Rev. 04/10) Application for a Search Warrant (Page 1)

UNITED STATES DISTRICT COURT
for the
Northern District of New York



1:18-MJ-380(CFH)

In the Matter of the Search of)
(Briefly describe the property to be searched)
(or identify the person by name and address)) Case No.
One (1) rose gold Apple iPhone 6s Plus in a)
multi-colored "Supreme" case;)
)
One (1) black Apple iPhone 6 in a black case;)
)
One (1) black Samsung Galaxy S9 smartphone in)
a blue/clear case; and)
)
One (1) white Samsung Galaxy smartphone in a)
black silver case.)
)
CURRENTLY LOCATED AT THE)
WATERVLIET POLICE DEPARTMENT, 2 15th)
STREET WATERVLIET, NEW YORK)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:
(identify the person or describe the property to be searched and its given location):

See Attachment A.

located in the Northern District of New York, there is now concealed
(identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841(a)(1), 841(b)(1)(B) and 846	Conspiracy to Possess with Intent to Distribute and to Distribute a Controlled Substance

The application is based on these facts:

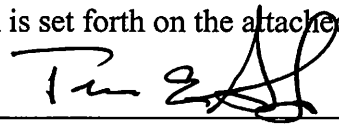
See attached affidavit.

AO 106 (Rev. 04/10) Application for a Search Warrant (Page 2)

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days):

is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



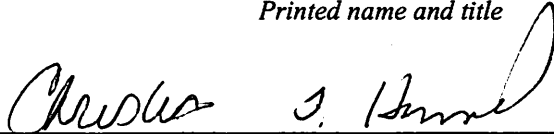
Applicant's signature

DEA Special Agent Terrance E. Dunlap

Printed name and title

Sworn to before me and signed in my presence.

Date: July 2, 2018



Judge's signature

City and State: Albany, NY

Hon. Christian F. Hummel, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK**

IN THE MATTER OF THE APPLICATION
FOR A SEARCH WARRANT FOR THE
FOLLOWING ELECTRONIC DEVICES:

One (1) rose gold Apple iPhone 6s Plus in a
multi-colored “Supreme” case;

One (1) black Apple iPhone 6 in a black case;

One (1) black Samsung Galaxy S9 smartphone
in a blue/clear case; and

One (1) white Samsung Galaxy smartphone in
a black silver case;

CURRENTLY LOCATED AT THE
WATERVLIET POLICE DEPARTMENT, 2
15th STREET WATERVLIET, NEW YORK.

Case No. 1:18-MJ-357 (CFH)

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Terrance E. Dunlap, a Special Agent with the Drug Enforcement Administration (“DEA”), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property — one (1) rose gold Apple iPhone 6s Plus in a mutli-colored “Supreme” case; one (1) black Apple iPhone 6 in a black case; one (1) black Samsung Galaxy S9 smartphone in a blue/clear case; and one (1) white Samsung Galaxy smartphone in a black silver case— hereinafter the “Devices,”

which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with DEA, duly appointed according to law and acting as such, I am an “investigative or law enforcement officer” within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516.

3. I have been so employed for approximately nineteen years. I am currently assigned to investigate illicit drug trafficking organizations in and around Albany, New York and the greater Capital District area. As a DEA Special Agent, I received sixteen (16) weeks of training at the DEA Academy in Quantico, Virginia, where I became familiar with how controlled substances are consumed, manufactured, packaged, marketed and distributed. During my career, I have participated in hundreds of investigations of alleged criminal violations of the Controlled Substances Act.

4. I have received training pertaining to the investigation of various crimes which arise from drug trafficking. I have participated in the execution of search warrants for controlled substances, the proceeds of drug trafficking and the documentary evidence of drug trafficking. I have conducted surveillances in connection with drug investigations as well as in response to court authorized wire intercepts. My experience as a Special Agent with the DEA, my participation in the investigations of both domestic and international drug trafficking organizations, my conversations with known drug traffickers, my conversations with other Special Agents of the DEA familiar with drug trafficking and money laundering, and my training and experience form the basis of my opinions and conclusions set forth below.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. The property to be searched is:

- (a) One (1) rose gold Apple iPhone 6s Plus in a multi-colored “Supreme” case;
- (b) One (1) black Apple iPhone 6 in a black case;
- (c) One (1) black Samsung Galaxy S9 smartphone in a blue/clear case; and
- (d) One (1) white Samsung Galaxy smartphone in a black silver case;

collectively and hereinafter the “Devices.” The Devices are currently in evidence storage at the Watervliet Police Department located at 2 15th Street Watervliet, New York.

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically-stored data particularly described in Attachment B.

INVESTIGATION & PROBABLE CAUSE

Controlled Purchase of Heroin from SOTO – June 1, 2018

8. On or about June 1, 2018, under the direction of law enforcement, a confidential source (“CS”)¹ communicated with Eric SOTO via text, and inquired about the availability of heroin. SOTO agreed to sell CS an amount of heroin in exchange for \$6,800. CS directed

¹ CS has received or will receive monetary compensation from DEA, as well as receiving compensation for minor expenses from a local police department, in exchange for his/her cooperation with this investigation. Previously, CS has cooperated with law enforcement to avoid potential charges in New York state court arising from his/her own heroin sales activity. CS has a criminal history that includes arrests for drug trafficking, and a felony conviction for grand larceny (2006).

SOTO to meet him/her in the parking lot of a Price Chopper in Watervliet, New York. Prior to the meeting, CS and his/her vehicle was searched for money and/or contraband with negative results, and CS was provided with \$6,800 in transcribed U.S. currency to purchase heroin from SOTO. CS was also fitted with transmitting and recording devices.

9. On June 1, 2018, at approximately 12:56 p.m., CS parked in the Watervliet Price Chopper parking lot. Around the same time, SOTO exited a blue Mercedes Benz SUV with New York registration GPR-2936, also parked in the lot, and entered CS's vehicle. The interaction inside CS' vehicle was video- and audio-recorded. At approximately 1:02 p.m., SOTO exited CS' vehicle and re-entered the blue Mercedes Benz SUV, and left the area.

10. Law enforcement agents followed CS back to a pre-determined location. Upon reaching the pre-determined location, law enforcement searched CS and his/her vehicle, and recovered the recording device, and a clear plastic baggie containing a tan powder substance weighing approximately 100 grams, which appeared to be heroin. The substance was not field-tested as CS reported that SOTO told him/her that it possibly contained fentanyl, and DEA policy prohibits field-testing suspected narcotics which agents have reason to believe may contain fentanyl. Confirmatory lab results are pending.

Controlled Purchase of Heroin from SOTO – June 15, 2018

11. On or about June 14 and 15, 2018, under the direction of law enforcement, CS communicated with SOTO via text, and inquired about the availability of heroin and Oxycotin. SOTO agreed to sell CS an amount of heroin and oxycodone pills in exchange for \$14,425. CS directed SOTO to meet him/her in the parking lot of the Colonie Center mall in Colonie, New York. Prior to the meeting, CS and his/her vehicle was searched for money and/or contraband

with negative results, and CS was provided with \$14,425 in transcribed U.S. currency to purchase heroin from SOTO. CS was also fitted with transmitting and recording devices.

12. On June 15, 2018, at approximately 1:37 p.m., CS parked in the Watervliet Price Chopper parking lot. Around the same time, SOTO exited a blue Mercedes Benz SUV with New York registration GPR-2936, also parked in the lot, and entered CS's vehicle. The interaction inside CS' vehicle was video- and audio-recorded. At approximately 1:44 p.m., SOTO exited CS' vehicle and re-entered the blue Mercedes Benz SUV, and left the area.

13. Law enforcement agents followed CS back to a pre-determined location. Upon reaching the pre-determined location, law enforcement searched CS and his/her vehicle, and recovered the recording device, and a clear plastic baggie containing a tan powder substance weighing approximately 200 grams, which appeared to be heroin. The substance was not field-tested as CS previously reported that SOTO told him/her that the heroin possibly contained fentanyl, and DEA policy prohibits field-testing suspected narcotics which agents have reason to believe may contain fentanyl. Confirmatory lab results are pending.

Arrest and Search of SOTO and LOPEZ DIETSCH – June 22, 2018

14. On or about June 21 and 22, 2018, under the direction of law enforcement, CS communicated with SOTO via text, and inquired about the availability of heroin. SOTO agreed to sell CS an amount of heroin and oxycodone pills in exchange for \$40,450. CS directed SOTO to meet him/her in the parking lot of the Crossgates Mall in Guilderland, New York.

15. On June 22, 2018, at approximately 1 p.m., CS received a text from SOTO advising CS that SOTO was at Crossgates Mall. Surveillance units were dispatched to the vicinity of Crossgates Mall. Members of the surveillance teams were able to locate SOTO's

vehicle, which has been previously identified as a Blue Mercedes Benz SUV with New York registration GPR-2936.

16. At approximately 1:44 p.m., SOTO and an unidentified male - later identified as Harold LOPEZ DIETSCH - exited the Crossgates Mall, and entered into the Blue Mercedes Benz SUV, as observed by members of the surveillance team. Around the same time, CS contacted SOTO and advised SOTO that CS was approaching the mall. SOTO advised CS to drive to the front of the mall's Best Buy entrance. CS parked in front of Best Buy entrance, however after a few minutes SOTO advised CS to drive to the vicinity of the mall's Forever 21 entrance. CS arrived near the Forever 21 entrance, and was again instructed by SOTO to relocate, this time to the vicinity of the mall's Pottery Barn entrance.

17. When CS's vehicle approached the vicinity of the mall's Pottery Barn entrance, LOPEZ DIETSCH exited the vehicle and appeared to maintain counter-surveillance for SOTO near the flagpole at the mall's Pottery Barn entrance, as observed by members of the surveillance team. SOTO then exited the Mercedes Benz SUV carrying what appeared to be a black and white striped bag.

18. SOTO was arrested by members of the surveillance team as he walked in the direction of CS's vehicle in the mall parking lot. At the same time, LOPEZ DIETSCH fled into the mall where he was arrested without incident. SOTO's bag was searched incident to the arrest and, *inter alia*, agents recovered two clear plastic baggies containing a tan powder substance weighing a total of approximately 600 grams, which appeared to be heroin. The substance was not field-tested as CS previously reported that SOTO told him/her that the heroin possibly contained fentanyl, and DEA policy prohibits field-testing suspected narcotics which agents have

reason to believe may contain fentanyl. Confirmatory lab results are pending. SOTO's bag also contained a clear plastic baggie containing a quantity of suspected Oxycontin pills.

The Devices

19. After being detained, LOPEZ-DIETSCH was searched incident to arrest, and one (1) rose gold Apple iPhone 6s Plus in a multi-colored "Supreme" case, and one (1) black Apple iPhone 6 in a black case were recovered recovered from his person. Both Apple iPhones were "locked," but were equipped with TouchID buttons allowing access to their authorized user. After being detained, SOTO was searched incident to arrest, and one (1) black Samsung Galaxy S9 smartphone in a blue/clear case; and one (1) white Samsung Galaxy smartphone in a black silver case from his person.

20. The Devices are currently in storage at the Watervliet Police Department located at 2 15th Street Watervliet, New York. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of DEA.

Traffickers of Controlled Substances

21. In my experience and training, and in the experience and training of the agents and investigators with whom I am working:

- a. Individuals involved in the unlawful importation and distribution of controlled substances including marijuana (hereafter "drug traffickers") often maintain records, receipts, notes, ledgers, airline tickets, money orders and other papers relating to the acquisition, importation, transportation, possession, sale and/or distribution of controlled substances.

- b. These individuals often utilize communication devices such as cell phones, tablets and computers to communicate regarding their efforts and to coordinate their shipments. These devices often provide large amounts of useful information regarding the conspiracy which can often be recovered even if the user attempts to delete or destroy the data on the device.
- c. These books, records, receipts, notes, ledgers, etc., are often maintained among the drug trafficker's personal property in traditional paper form, or stored electronically on computers or other electronic storage devices. This includes the vouchers/receipts from negotiable instruments such as money orders.
- d. It is common for drug traffickers to secrete contraband and drug paraphernalia, proceeds of drug sales and records of drug transactions in secure locations within their personal property for ready access and to conceal them from law enforcement authorities.
- e. Drug traffickers attempt to legitimize their profits from the sale of drugs. To accomplish this goal, drug traffickers use, among other methods: 1) banks, foreign and domestic, and their attendant services; 2) securities; 3) cashier's checks; 4) money drafts; 5) letters of credit; 6) real estate; and 7) businesses real and fictitious.
- f. Depending on the scale of their drug distribution business, persons involved in drug trafficking may conceal in their personal property caches of drugs, large amounts of currency, financial instruments, precious metals, jewelry and other items of value that are the proceeds of drug transactions and evidence of financial

transactions, relating to obtaining, transferring, secreting or spending of large sums of money made from engaging in drug trafficking activities.

- g. Persons engaged in money laundering frequently retain records of their transactions within their residence, place of business, rented storage units, vehicles, or other places under their control or where they have regular access. These records may be in the form of written notes and correspondence, receipts, negotiated instruments, contracts, bank statements and other records. Records of this kind are also often stored on computer media.
- h. Individuals who amass proceeds from illegal activities, including money laundering, routinely attempt to further that conduct and/or conceal the existence and source of their funds by engaging in financial transactions with domestic and foreign institutions, and others, through all manner of financial instruments, including cash, cashier's checks, money drafts, traveler's checks, wire transfers, etc. Records of such instruments are routinely maintained at the individual's residence or place of business or other place to which they have continual access, including phones.

22. In my experience and training, and in the experience of the agents and investigators with whom I am working, individuals suspected of drug trafficking and money laundering crimes often (knowingly or unknowingly) keep evidence of their crimes and may do so even after they become aware of a possible investigation. This is because:

- a. Persons engaged in money laundering often maintain records for long periods of time. Although this is true for paper records, it is especially true for records kept in digital format. Digital storage does not require physical storage space and

because digital storage space, whether in the form of computer hard drives, external hard drives, flash memory, digital video disks, compact disks, or other forms of digital storage media, is inexpensive and easy to purchase and maintain, it is not uncommon for persons engaged in longer-term financial crimes to maintain records in both paper and digital form for a number of years.

- b. There are many reasons why criminal offenders maintain evidence for long periods of time. The evidence may be innocuous at first glance -- e.g. financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, checkbooks, video and photographs, utility records, ownership records, letters and notes, and financial records, keys to safe deposit boxes -- but have significance and relevance when considered in light of other evidence. The criminal offender may no longer realize s/he still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that s/he has deleted, hidden, or further destroyed any computer-related evidence that may actually be retrieved by a trained forensic computer expert.

23. Based on the above, I believe there is probable cause to believe the Devices contain evidence and/or instrumentalities of violations of Title 21, United States Code, Sections 841(a)(1), 841(b)(1)(B) and 846 (Conspiracy to Possess with Intent to Distribute and to Distribute a Controlled Substance), by knowingly and intentionally possessing with the intent to distribute and distributing 100 grams or more of a substance that contained a detectable amount of heroin.

TECHNICAL TERMS

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- d. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data

and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device

- f. Removable Storage Media: include various types of flash memory cards or miniature hard drives. Removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

25. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and removable electronic storage for digital files, including audio and video files, produced by digital cameras or downloaded from the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

27. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is

typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

APPLE IPHONES WITH TOUCH ID

31. Beginning with the release of iOS 8 (the operating system for Apple mobile devices) in September 2014, Apple no longer has a key to decrypt these devices. Thus, even with a properly authorized search warrant to gain access to the content of an iOS device, there is no feasible way for the government to search the device.

32. I know from my training and experience and my review of publicly available materials published by Apple that those Apple devices can enable what is referred to as "Touch ID," a feature that recognizes up to five fingerprints designated by the authorized user of the iPhone. A Touch ID sensor, a round button on the iPhone or iPad, can recognize fingerprints. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require. The Touch ID feature only permits up to five attempts with a fingerprint before the device will require the user to enter a passcode.

33. Furthermore, for devices running iOS 9.2.1 or lower, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; and for devices running iOS 9.3 and later, the Touch ID cannot be

used if the device passcode/password has not been used to unlock the device in the last six days and Touch ID has not unlocked the device in the last eight hours. Similarly, Touch ID will not allow access if the device has been turned off or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful.

34. For these reasons, it is necessary to use the fingerprints and thumbprints of LOPEZ-DIETSCH to attempt to gain access to the two Apple iPhones recovered from LOPEZ-DIETSCH. The government may not be able to obtain the contents of the Apple iPhones if those fingerprints are not used to access the locked devices by depressing them against the Touch ID buttons. Although I do not know which finger or fingers are authorized to access on either Apple iPhone, and only five attempts are permitted, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for Touch ID, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password. No damage to the device would result from failed attempts.

35. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of LOPEZ-DIETSCH to the two recovered Apple iPhones for the purpose of attempting to unlock the devices via Touch ID in order to search the contents as authorized by this warrant.

///

///

///

///

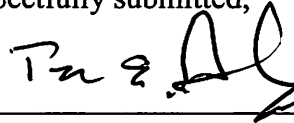
///

///

CONCLUSION

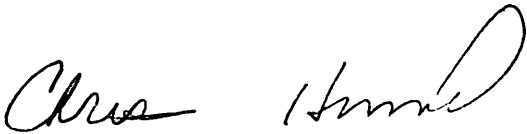
36. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Terrance E. Dunlap
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me
On July 2, 2018:



HON. CHRISTIAN F. HUMMEL
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is:

- (a) one (1) rose gold Apple iPhone 6s Plus in a mutli-colored “Supreme” case;
- (b) one (1) black Apple iPhone 6 in a black case;
- (c) one (1) black Samsung Galaxy S9 smartphone in a blue/clear case; and
- (d) one (1) white Samsung Galaxy smartphone in a black silver case;

collectively and hereinafter the “Devices.” The Devices are currently in evidence storage at the Watervliet Police Department located at 2 15th Street Watervliet, New York.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically-stored information described in Attachment B.

ATTACHMENT B

The items to be searched for and seized are:

All records on the Devices described in Attachment A that relate to violations of Title 21, United States Code, Sections 841(a)(1), 841(b)(1)(B) and 846 (Conspiracy to Possess with Intent to Distribute and to Distribute a Controlled Substance):

Computers and Electronic Media

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and electronic media will be conducted in accordance with the affidavit submitted in support of this warrant.
2. Computer hardware, meaning any and all computer equipment, including any electronic storing devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as thumb drives, flash drives, SD (secure digital) cards, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical and compact storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing, or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).
3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems, software, application software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.
5. Computer passwords and data security devices, meaning any devices, programs, or data, whether themselves in the nature of hardware or software, that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data

records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips and circuit boards); passwords; data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data, or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents and materials referencing or relating to the above described offenses. Such records, documents or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing or typing); any electrical, electronic or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as thumb drives, flash drives, sd (secure digital) cards, floppy diskettes, hard disks, CD-ROMs, DVDs, optical disks, printer buffers, soft cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.
7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), or any computer or computer system. The form that such information might take includes, but is not limited to, thumb drives, flash drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, DVDs, video cassettes, and other media capable of storing magnetic or optical coding.
8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or Internet-based communications, or which contains material or data, obtained through computer or Internet-based communications, including data in the form of electronic records, documents and materials, including those used to facilitate interstate communications, included but not limited to telephone (including mobile telephone) and Internet Service Providers. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding, on computer media, or on media capable of being read by a computer or computer-related equipment, such as thumb drives, flash drives, SD (secure digital) cards, fixed disks, external hard disks, removable hard disk cartridges, CDs, DVDs, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, or other memory storage devices.

Documents, Records and Evidence

9. Records of personal and business activities relating to the operation and ownership of the Devices.
10. Any records or documents pertaining to accounts held with Internet Service Providers or of Internet use.
11. Records of address or identifying information for the target of the investigation and any personal or business contacts or associates of his, (however and wherever written, stored or maintained), including contact lists, buddy lists, email lists, ICQ addresses, IRC names (a.k.a., "Nics"), user ID's, eID's (electronic ID numbers) and passwords.
13. Documents and records regarding the ownership and/or possession of the Devices.
15. Evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software, and evidence of the lack of such malicious software.
16. Evidence indicating how and when the Devices were accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user.
17. Evidence of the attachment to an item of electronic media of other storage devices or similar containers of electronic evidence.
19. Evidence of the times any item of electronic media was used.
20. Passwords, encryption keys, and other access devices that may be necessary to access any electronic media.
21. Documentation and manuals that may be necessary to access seized electronic media or to conduct a forensic examination of the media.
22. Records of or information about Internet Protocol addresses used by seized electronic media, as well as records of or information about the media's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
23. Contextual information necessary to understand the evidence described in this attachment.

Materials Relating to Trafficking in Controlled Substances

24. Any and all chats, chat logs, emails, and other text documents, describing or relating to drug trafficking.
26. Any and all address books, names, and lists of names and addresses of co-conspirators engaged in drug trafficking.
27. Records, relating to the source of proceeds deposited to personal and/or corporate bank accounts.
28. Records relating to deposits to personal and/or corporate bank accounts and expenditures of money and wealth, to wit: money orders, wire transfers, cashier checks and receipts, bank statements, passbooks, checkbooks, and check registers.
29. Records related to the purchase of personal assets, including but not limited to real estate, vehicles, jewelry and boats.
30. Records related to foreign or domestic travel to include but not limited to passports, documentation of travel destinations and time periods, and any and all records of expenses related to travel.
31. Records relating to the shipment, both inbound and outbound, of controlled substances. This shall include, but is not limited to, packaging, packing slips, packaging materials and packaging supplies, used in the shipment of sending and/or receiving controlled substances. This shall also include proof of past shipments such as receipts and other records and indicia of mailings.

Where Thumbprints Required to Search Devices

32. During the execution of the search of the Apple iPhone devices described in Attachment A, law enforcement personnel are authorized to press or swipe the fingers (including thumbs) of LOPEZ-DIETSCH, who is believed by law enforcement to be a user of the devices for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.